Journal of Pure and Applied Algebra 72 (1991) 251–263
North-Holland

Insoluble groups with the rewriting property $\mathbf{P}_8$

Russell D. Blyth

Department of Mathematics and Computer Science, Saint Louis University, St. Louis, MO 63103, USA

Derek J.S. Robinson

Department of Mathematics, University of Illinois in Urbana-Champaign, Urbana, IL 61801, USA

Communicated by K.W. Gruenberg
Received 16 January 1990

Abstract

Blyth, R.D. and D.J.S. Robinson, Insoluble groups with the rewriting property $\mathbf{P}_8$, Journal of Pure and Applied Algebra 72 (1991) 251–263.

Let n be an integer greater than 1, and let G be a group. An n-tuple $x_1, x_2, \ldots, x_n$ of elements of G is called *rewritable* if there is a nontrivial permutation π of $\{1, 2, \ldots, n\}$ such that $x_1x_2\cdots x_n = x_{\pi(1)}x_{\pi(2)}\cdots x_{\pi(n)}$. The group G is said to have the *rewriting property* $\mathbf{P}_n$ if every n-tuple of G is rewritable.

The authors have previously shown that all groups with $\mathbf{P}_7$ are soluble, whereas the alternating group A_5 has $\mathbf{P}_8$. Thus the least n for which $\mathbf{P}_n$ contains a nonabelian simple group is 8. In this article the authors confirm conjectures of R. Brandl concerning the structure of insoluble groups with $\mathbf{P}_8$. In particular, let G be an insoluble group. Then G has the rewriting property $\mathbf{P}_8$ if and only if it is a semidirect product $H \ltimes K$ where H is abelian, K is isomorphic with the alternating group of degree 5, and $|H:C_H(K)| = 1$ or 2.

1. Introduction

Let n be an integer greater than 1, and let G be a group. An n-tuple $x_1, x_2, \ldots, x_n$ of elements of G is called *rewritable* if there is a nontrivial permutation π of $\{1, 2, \ldots, n\}$ such that

$$x_1x_2\cdots x_n = x_{\pi(1)}x_{\pi(2)}\cdots x_{\pi(n)}.$$

The group G is said to have the *rewriting property*

$$\mathbf{P}_n,$$

or to be *totally n-rewritable*, if every n-tuple of G is rewritable. Recently there has been a good deal of interest in rewriting properties, the original motivation coming from automata theory. A basic theorem due to Curzio, Longobardi, Maj and Robinson [8] characterizes groups that have $\mathbf{P}_n$ for some n as precisely the finite-by-abelian-by-finite groups. For a survey of the subject up to 1987 the reader may consult [3].

In a recent article [4] the authors proved that all groups with $\mathbf{P}_7$ are soluble, whereas the alternating group A_5 has $\mathbf{P}_8$. Thus the least n for which $\mathbf{P}_n$ contains a nonabelian simple group is 8. In a private communication R. Brandl has conjectured that A_5 is the only nonabelian simple group with $\mathbf{P}_8$; he further suggested that insoluble groups with $\mathbf{P}_8$ might have a restricted structure. Our purpose here is to confirm Brandl's conjectures by establishing the following result:

Theorem. *Let G be an insoluble group. Then G has the rewriting property $\mathbf{P}_8$ if and only if it is a semidirect product $H \ltimes K$ where H is abelian, K is isomorphic with the alternating group of degree 5, and $|H : C_H(K)| = 1$ or 2.*

As an immediate consequence of the theorem one obtains a new characterization of A_5.

Corollary 1. *The only nontrivial perfect group with the property $\mathbf{P}_8$ is the alternating group A_5.* □

So far as soluble groups with $\mathbf{P}_8$ are concerned, all that is known is that their derived lengths cannot exceed 10 (see [11]), a bound that is unlikely to be best possible. Recently a very complex classification of groups with $\mathbf{P}_4$—all of which are soluble of course—has been given by Longobardi, Maj and Stonehewer [12]. In view of this it seems unlikely that complete information about soluble groups with $\mathbf{P}_8$ is attainable.

To prove the Theorem we need the classification of finite simple groups, and also a good deal of information about subgroups of simple groups of Lie type. Another feature of the proof is an extensive amount of electronic computation, which is employed to show that various simple groups of low order do not have $\mathbf{P}_8$, and that the symmetric group S_5 has $\mathbf{P}_8$. The need for these powerful tools is mainly due to the difficulty of making direct deductions from rewriting properties.

2. Simple groups with $\mathbf{P}_8$

The first step in the proof of the Theorem consists in identifying those simple groups that have $\mathbf{P}_8$.

Proposition 2. *The only nonabelian simple group with the property $\mathbf{P}_8$ is the alternating group A_5.*

It is a consequence of the structure theorem for groups with a rewriting property $\mathbf{P}_n$ that a simple group with $\mathbf{P}_8$ is necessarily finite [8]. Thus, assuming the proposition to be false, we seek to identify groups that are counterexamples of minimum order. In such a group each proper nonabelian simple section is of type A_5. Thus we need to determine the finite simple groups with this property, which is done in the next result.

Proposition 3.[1] *The finite nonabelian simple groups all of whose proper nonabelian simple sections are isomorphic with* A_5, *are precisely*:

$PSL(2, 2^m)$, $m = 4$ *or a prime* ;

$PSL(2, 3^m)$, $PSL(2, 5^m)$, m *a prime* ;

$PSL(2, p)$, p *a prime* ≥ 7 ;

$PSL(3, 3)$, $PSL(3, 5)$, $PSU(3, 4)$ *and*

$Sz(2^m)$, m *an odd prime* .

Proof. Let G be a finite nonabelian simple group with the property stated. By the classification G is an alternating group, a group of Lie type or a sporadic group. Since A_n occurs as a subgroup of A_{n+1}, the only alternating groups that qualify as G are $A_5 \cong PSL(2, 4)$ and $A_6 \cong PSL(2, 9)$, which are on the list. Also G cannot be a sporadic group, as can be seen from an inspection of maximal subgroups listed in the ATLAS [7].

Suppose now that G is a simple group of Lie type[2]. If G is a Chevalley group, then it has a subgroup of type $SL(2, q)$ or $PSL(2, q)$ where q is the field parameter of G; indeed such a subgroup is generated by the root subgroups X_r and X_{-r} where r is a positive root (see [6, p. 88]). Hence either $G \cong PSL(2, q)$ or $q \leq 5$ in this case. If G is a unitary group, there is also a subgroup of type $SL(2, q)$ or $PSL(2, q)$ arising from root subgroups (see [2, p. 251]) and we reach the same conclusion. Thus again $q \leq 5$. After these general observations we shall discuss the different types of group separately.

(i) $G \cong PSL(n, q)$. Since $PSL(n-1, q)$ occurs as a section of $PSL(n, q)$, we must have $n = 2$ or 3. If $G \ncong PSL(2, q)$, then $n = 3$ and $q \leq 5$. But $PSL(3, 2) \cong PSL(2, 7)$ and $PSL(3, 4)$ has a subgroup of type A_6. Thus we are left with just $PSL(2, q)$, $PSL(3, 3)$ and $PSL(3, 5)$. The restrictions on q follow from the list of subgroups of $PSL(2, q)$ in [9, p. 213].

[1] We understand that this result has been found independently by M. Döll.

[2] J.H. Walter has pointed out that if the rank of the simple group of Lie type is not too small, this result may also be obtained by inspecting an appropriate Levi subgroup of a parabolic subgroup of each group.

[3] For this and other low degree isomorphisms, see [1, p. 253].

(ii) $G \cong P\mathrm{sp}(2n, q)$. We may assume that $n > 1$ since $P\mathrm{sp}(2, q) \cong P\mathrm{SL}(2, q)^3$. Because $P\mathrm{sp}(2n-2, q)$ is isomorphic with a section of $P\mathrm{sp}(2n, q)$, we must have $n = 2$. The possibilities that remain are $P\mathrm{sp}(4, 3)$, $P\mathrm{sp}(4, 4)$ and $P\mathrm{sp}(4, 5)$, all of which have a subgroup of type A_6 (see the ATLAS). So no new groups arise.

(iii) $G \cong P\mathrm{SU}(n, q)$. Since $P\mathrm{SU}(2, \mathrm{q}) \cong P\mathrm{SL}(2, q)$, we can assume that $n > 2$. Also $P\mathrm{SU}(n-2, q)$ occurs as a section of $P\mathrm{SU}(n, q)$, as may be seen from the hermitian form; therefore $n = 3$ or 4. Keeping in mind that $P\mathrm{SU}(3, 2)$ is not simple and $P\mathrm{SU}(4, 2) \cong P\mathrm{sp}(4, 3)$, we conclude that only $P\mathrm{SU}(3, 3)$, $P\mathrm{SU}(3, 4)$, $P\mathrm{SU}(3, 5)$, $P\mathrm{SU}(4, 3)$, $P\mathrm{SU}(4, 4)$ and $P\mathrm{SU}(4, 5)$ need be checked. According to the ATLAS, the three groups $P\mathrm{SU}(3, 3)$, $P\mathrm{SU}(3, 5)$ and $P\mathrm{SU}(4, 3)$ do not qualify. Also $P\mathrm{SU}(4, q) \cong P\Omega^-(6, q)$, which has a section of type $P\Omega^-(4, q) \cong P\mathrm{SL}(2, q^2)$. Hence $P\mathrm{SU}(4, 4)$ and $P\mathrm{SU}(4, 5)$ are also excluded; only $P\mathrm{SU}(3, 4)$ remains.

(iv) $G \cong P\Omega^{\pm}(n, q)$. In view of the isomorphisms $P\Omega(3, q) \cong P\mathrm{SL}(2, q)$, $P\Omega^+(4, q) \cong P\mathrm{SL}(2, q) \times P\mathrm{SL}(2, q)$ and $P\Omega^-(4, q) \cong P\mathrm{SL}(2, q^2)$, we can assume that $n \geq 5$. An examination of the various quadratic forms that define G shows that $P\Omega^{\epsilon}(n-2, q)$ occurs as a section of $P\Omega^{\epsilon}(n, q)$. Therefore $n = 5$ or 6. But $P\Omega(5, q) \cong P\mathrm{sp}(4, q)$, $P\Omega^+(6, q) \cong P\mathrm{SL}(4, q)$ and $P\Omega^-(6, q) \cong P\mathrm{SU}(4, q)$. Hence no new groups arise.

(v) $G \cong \mathrm{Sz}(2^m)$, m odd. Since Sz(2) is the Frobenius group of order 20, we may assume that $m > 1$. If $m = st$, where $s > 1$ and $t > 1$, then G contains the simple group $\mathrm{Sz}(2^s)$ [15].

(vi) $G \cong {}^2F_4(2^m)$, m odd. By [16, p. 210–05], G has a subgroup of type $P\mathrm{SL}(2, 2^m)$. Hence $m = 1$. Although ${}^2F_4(2)$ is not simple, its commutator subgroup ${}^2F_4(2)'$ of index 2 is simple. According to the ATLAS, ${}^2F_4(2)'$ has a subgroup of type $P\mathrm{SL}(3, 3)$.

(vii) $G \cong {}^2G_2(3^m)$, m odd. By [10, p. 292] G has a subgroup of type $P\mathrm{SL}(2, 3^m)$, so $m = 1$; but then $G = {}^2G_2(3)$ is not simple. However, ${}^2G_2(3)'$ is simple and is isomorphic to $P\mathrm{SL}(2, 8)$. Again no new examples arise.

(viii) G an exceptional group. According to a table in [14, p. 363], the following groups have proper nonabelian simple sections other than A_5:

$$E_6(q), \quad E_7(q), \quad E_8(q),$$
$$F_4(q), \quad G_2(q), \quad {}^3D_4(q), \quad \text{and} \quad {}^2E_6(q) \text{ for } q > 2.$$

Finally, ${}^2E_6(2)$ has a subgroup of type $P\mathrm{SL}(3, 2)$, by the ATLAS. So all the exceptional groups can be eliminated.

Finally the groups on our list do have the property claimed, as may be seen from [9, 15] and the ATLAS. □

Next we recall a key result from [4] which will be used to produce a finite set of possible counterexamples to Proposition 2.

Proposition 4. (i) *If* $PSL(2, q)$ *has the property* $\mathbf{P}_n$, *then* $q \leq \frac{1}{2} + \sqrt{2(n-1)(n-1)! + \frac{1}{4}}$.

(ii) *If* $Sz(q)$ *has the property* $\mathbf{P}_n$, *then* $q \leq \sqrt{(n-1)(n-1)! - 1}$. □

Proof of Proposition 2. It was shown in [4] that the alternating group A_5 has $\mathbf{P}_8$. Conversely, let G be a finite nonabelian simple group with the property $\mathbf{P}_8$ which has smallest order subject to not being isomorphic with A_5. Then every proper nonabelian simple section is of type A_5. Combining Propositions 3 and 4, we conclude that G must be one of the following groups:

(i) $PSL(2, 2^m)$, $m = 3, 4, 5, 7$,

(ii) $PSL(2, 3^m)$, $m = 2, 3, 5$,

(iii) $PSL(2, 25)$, $PSL(2, 125)$,

(iv) $PSL(2, p)$, p a prime, $7 \leq p \leq 263$,

(v) $PSL(3, 3)$, $PSL(3, 5)$,

(vi) $PSU(3, 4)$,

(vii) $Sz(2^m)$, $m = 3, 5$ or 7.

Thus we have a list of 68 simple groups. The proof is completed by exhibiting a nonrewritable 8-tuple in each group, a task that must, of course, be accomplished by electronic computation.

We comment briefly on the computational methodology. In the case of the groups $PSL(2, 9)$, $PSL(2, 17)$, $PSL(2, 23)$ and $PSL(3, 3)$ a computer search using CAYLEY on a SUN 3/50 extended 7-tuples found in [4] to nonrewritable 8-tuples. This procedure becomes impracticable for groups of large order. The groups $PSL(2, 7)$, $PSL(2, 11)$, $PSL(2, 13)$, $PSL(2, 16)$ and $PSL(2, 19)$ were dealt with by using a specially written PASCAL program to generate nonrewritable tuples; the underlying algorithm is described in [4]. Here a Micro VAX II was used. The group $PSL(2, 8)$ was handled by a similar program written in C++, running on a Multimax (see [13]).

Nonrewritable 8-tuples were found in the remaining 58 groups by using CAYLEY on a SUN 3/50 to generate and test 8-tuples by using the random element function. Usually a nonrewritable 8-tuple appeared fairly soon, although in the case of $PSL(2, 27)$ the 151st 8-tuple generated was the first that failed to rewrite. The random element method is, not surprisingly, only effective for groups of quite large order.

The following is a list of nonrewritable 8-tuples in low-order groups, where they are harder to find. The authors have a complete list of nonrewritable 8-tuples for all 68 simple groups. In the case of the linear groups over nonprime fields the irreducible polynomial determining the field is given. For the groups $PSL(2, q)$, q odd, matrices are to be taken modulo the centre of $SL(2, q)$.

(1) $PSL(2, 7)$.

$$\begin{bmatrix}1&0\\1&1\end{bmatrix},\begin{bmatrix}2&0\\0&4\end{bmatrix},\begin{bmatrix}1&0\\2&1\end{bmatrix},\begin{bmatrix}0&1\\6&1\end{bmatrix},$$
$$\begin{bmatrix}1&5\\0&1\end{bmatrix},\begin{bmatrix}1&6\\2&6\end{bmatrix},\begin{bmatrix}2&1\\1&1\end{bmatrix},\begin{bmatrix}2&6\\1&0\end{bmatrix}.$$

(2) $PSL(2, 8)$ (irreducible polynomial $x^3 + x^2 + 1$).

$$\begin{bmatrix}1&0\\1&1\end{bmatrix},\begin{bmatrix}1&1\\0&1\end{bmatrix},\begin{bmatrix}1&0\\x&1\end{bmatrix},\begin{bmatrix}1&1\\x^2&x^2+1\end{bmatrix},$$
$$\begin{bmatrix}1&0\\x+1&1\end{bmatrix},\begin{bmatrix}1&x\\0&1\end{bmatrix},\begin{bmatrix}1&0\\x^2&1\end{bmatrix},\begin{bmatrix}x^2+1&x+1\\x^2+x&x^2+1\end{bmatrix}.$$

(3) $PSL(2, 9) \cong A_6$.

$$(1,2)(3,4), (2,5)(3,4), (1,4)(2,3), (1,2,3,5,4),$$
$$(1,5,4,3,2), (2,4)(3,5), (1,3)(2,4), (1,6,4)(2,5,3).$$

(4) $PSL(2, 11)$.

$$\begin{bmatrix}1&0\\1&1\end{bmatrix},\begin{bmatrix}2&0\\0&6\end{bmatrix},\begin{bmatrix}1&0\\2&1\end{bmatrix},\begin{bmatrix}2&0\\5&6\end{bmatrix},$$
$$\begin{bmatrix}0&1\\10&0\end{bmatrix},\begin{bmatrix}1&0\\3&1\end{bmatrix},\begin{bmatrix}3&4\\7&6\end{bmatrix},\begin{bmatrix}1&0\\9&1\end{bmatrix}.$$

(5) $PSL(2, 13)$.

$$\begin{bmatrix}1&0\\1&1\end{bmatrix},\begin{bmatrix}2&0\\0&7\end{bmatrix},\begin{bmatrix}1&0\\2&1\end{bmatrix},\begin{bmatrix}2&0\\4&7\end{bmatrix},$$
$$\begin{bmatrix}0&1\\12&0\end{bmatrix},\begin{bmatrix}1&0\\3&1\end{bmatrix},\begin{bmatrix}5&0\\0&8\end{bmatrix},\begin{bmatrix}4&4\\7&4\end{bmatrix}.$$

(6) $PSL(2, 16)$ (irreducible polynomial $x^4 + x^3 + 1$).

$$\begin{bmatrix}1&0\\1&1\end{bmatrix},\begin{bmatrix}x&0\\0&x^3+x^2\end{bmatrix},\begin{bmatrix}1&0\\x&1\end{bmatrix},\begin{bmatrix}x&0\\x^2+1&x^3+x^2\end{bmatrix},$$
$$\begin{bmatrix}0&1\\1&0\end{bmatrix},\begin{bmatrix}1&0\\x+1&1\end{bmatrix},\begin{bmatrix}x&0\\x^3&x^3+x^2\end{bmatrix},\begin{bmatrix}x&1\\x+1&1\end{bmatrix}.$$

(7) $PSL(2, 17)$.

$$\begin{bmatrix}1&1\\0&1\end{bmatrix},\begin{bmatrix}9&9\\0&2\end{bmatrix},\begin{bmatrix}1&0\\1&1\end{bmatrix},\begin{bmatrix}13&13\\0&4\end{bmatrix},$$
$$\begin{bmatrix}9&0\\2&2\end{bmatrix},\begin{bmatrix}13&0\\4&4\end{bmatrix},\begin{bmatrix}6&6\\0&3\end{bmatrix},\begin{bmatrix}9&5\\9&7\end{bmatrix}.$$

(8) $PSL(2, 19)$.

$$\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix},\begin{bmatrix}2 & 0\\0 & 10\end{bmatrix},\begin{bmatrix}1 & 0\\2 & 1\end{bmatrix},\begin{bmatrix}2 & 0\\4 & 10\end{bmatrix},$$
$$\begin{bmatrix}1 & 0\\10 & 1\end{bmatrix},\begin{bmatrix}0 & 1\\18 & 0\end{bmatrix},\begin{bmatrix}1 & 0\\3 & 1\end{bmatrix},\begin{bmatrix}0 & 1\\18 & 2\end{bmatrix}.$$

(9) $PSL(2, 23)$.

$$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix},\begin{bmatrix}12 & 12\\0 & 2\end{bmatrix},\begin{bmatrix}6 & 6\\0 & 4\end{bmatrix},\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix},$$
$$\begin{bmatrix}6 & 0\\4 & 4\end{bmatrix},\begin{bmatrix}12 & 0\\2 & 2\end{bmatrix},\begin{bmatrix}8 & 8\\0 & 3\end{bmatrix},\begin{bmatrix}1 & 12\\2 & 2\end{bmatrix}.$$

(10) $PSL(2, 25)$ (irreducible polynomial $x^2 + x + 2$).

$$\begin{bmatrix}x^8 & 1\\x^2 & x^{21}\end{bmatrix},\begin{bmatrix}x^{15} & x^{11}\\x & 0\end{bmatrix},\begin{bmatrix}x^8 & x^4\\x^{10} & x^7\end{bmatrix},\begin{bmatrix}x^{17} & x^9\\x^{12} & x^6\end{bmatrix},$$
$$\begin{bmatrix}x^{14} & x^{14}\\x^{12} & x^{15}\end{bmatrix},\begin{bmatrix}x^{18} & 1\\x^8 & x^{10}\end{bmatrix},\begin{bmatrix}x^{21} & x^{13}\\x^{18} & 1\end{bmatrix},\begin{bmatrix}x^{11} & x^7\\x & x^{17}\end{bmatrix}.$$

(11) $PSL(2, 27)$ (irreducible polynomial $x^3 + 2x^2 + 1$).

$$\begin{bmatrix}x^{11} & x^{14}\\1 & x^{13}\end{bmatrix},\begin{bmatrix}x^{24} & x^9\\x^{15} & x^7\end{bmatrix},\begin{bmatrix}x^{11} & x^{25}\\x^8 & x^{18}\end{bmatrix},\begin{bmatrix}x^2 & x^{14}\\x^{23} & x^{25}\end{bmatrix},$$
$$\begin{bmatrix}x & x^{11}\\x^5 & x^{19}\end{bmatrix},\begin{bmatrix}x^{21} & x^{17}\\x^4 & x^{14}\end{bmatrix},\begin{bmatrix}x & x^{24}\\1 & x^4\end{bmatrix},\begin{bmatrix}x^{10} & x^9\\x & x^{20}\end{bmatrix}.$$

(12) $PSL(2, 29)$.

$$\begin{bmatrix}21 & 3\\12 & 28\end{bmatrix},\begin{bmatrix}8 & 19\\14 & 8\end{bmatrix},\begin{bmatrix}16 & 2\\6 & 28\end{bmatrix},\begin{bmatrix}24 & 6\\10 & 11\end{bmatrix},$$
$$\begin{bmatrix}8 & 17\\19 & 26\end{bmatrix},\begin{bmatrix}9 & 22\\1 & 9\end{bmatrix},\begin{bmatrix}1 & 12\\15 & 7\end{bmatrix},\begin{bmatrix}7 & 3\\10 & 21\end{bmatrix}.$$

(13) $PSL(2, 31)$.

$$\begin{bmatrix}6 & 14\\3 & 2\end{bmatrix},\begin{bmatrix}15 & 4\\20 & 24\end{bmatrix},\begin{bmatrix}10 & 0\\30 & 28\end{bmatrix},\begin{bmatrix}22 & 20\\3 & 7\end{bmatrix},$$
$$\begin{bmatrix}22 & 5\\7 & 27\end{bmatrix},\begin{bmatrix}23 & 30\\26 & 7\end{bmatrix},\begin{bmatrix}15 & 24\\17 & 12\end{bmatrix},\begin{bmatrix}6 & 28\\17 & 2\end{bmatrix}.$$

(14) $PSL(3, 3)$.

$$\begin{bmatrix}1 & 2 & 1\\0 & 1 & 1\\2 & 1 & 0\end{bmatrix},\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\2 & 1 & 1\end{bmatrix},\begin{bmatrix}1 & 0 & 0\\2 & 1 & 0\\1 & 1 & 1\end{bmatrix},\begin{bmatrix}1 & 1 & 2\\0 & 1 & 1\\0 & 0 & 1\end{bmatrix},$$

$$\begin{bmatrix}1&0&0\\1&1&0\\1&1&1\end{bmatrix},\begin{bmatrix}1&2&0\\0&1&1\\0&0&1\end{bmatrix},\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix},\begin{bmatrix}1&1&1\\1&2&0\\1&2&1\end{bmatrix}.$$

(15) $P\mathrm{SU}(3,4)$ (irreducible polynomial x^4+x+1).

$$\begin{bmatrix}x^{12}&0&x^{12}\\x&x^6&x\\x^4&x^7&x^6\end{bmatrix},\begin{bmatrix}x^7&0&0\\x^{14}&x^6&0\\x^{14}&x^4&x^2\end{bmatrix},\begin{bmatrix}x^{14}&x^9&x^5\\x^9&x^6&x^9\\x^6&x^{14}&x^3\end{bmatrix},\begin{bmatrix}x^{14}&x&x^{13}\\x^4&x^4&x^{11}\\x^{11}&x^{14}&x^4\end{bmatrix},$$
$$\begin{bmatrix}x^{11}&x^5&x^4\\x^{10}&x^7&x\\x^8&x^{13}&x^5\end{bmatrix},\begin{bmatrix}x^{12}&x^{13}&x^4\\x^9&x^5&x^5\\1&x^2&x^{11}\end{bmatrix},\begin{bmatrix}x^9&x^5&x^8\\x^{14}&x^3&x^4\\x^5&x^5&x^7\end{bmatrix},\begin{bmatrix}x^4&0&0\\x^5&x^{12}&0\\x^2&x&x^{14}\end{bmatrix}.$$

(16) $P\mathrm{SL}(2,32)$ (irreducible polynomial x^5+x^3+1).

$$\begin{bmatrix}x^{19}&x^5\\x^{24}&x^7\end{bmatrix},\begin{bmatrix}x^{23}&x^{15}\\x^{18}&x^5\end{bmatrix},\begin{bmatrix}x^{29}&x^4\\x^{29}&x^{30}\end{bmatrix},\begin{bmatrix}x^{18}&x^{15}\\x^{17}&x^{27}\end{bmatrix},$$
$$\begin{bmatrix}x^7&x^2\\x^{21}&x^4\end{bmatrix},\begin{bmatrix}x^{16}&x^4\\x^{18}&x^{30}\end{bmatrix},\begin{bmatrix}x^{24}&x^{20}\\x^{16}&x^{10}\end{bmatrix},\begin{bmatrix}x^5&x^7\\1&x^{11}\end{bmatrix}.\quad\square$$

3. Proof of the main result

Before commencing the proof we must give some preliminary results.

Proposition 5. (a) *The symmetric group S_5 has the property $\mathbf{P}_8$.*
(b) *The group* $\mathrm{SL}(2,5)$ *does not have the property $\mathbf{P}_8$.* □

Both statements are proved by machine computation. The proof of (a) requires a massive amount of computing power. The improved algorithm described by Robison was used with four SUN 3/60s running in parallel to produce the following data in approximately 11 CPU hours (see [13]); here $N(r)$ is the number of conjugacy classes of nonrewritable r-tuples in S_5.

r	2	3	4	5	6	7	8
$N(r)$	122	11,340	811,226	20,450,294	10,358,838	37,224	0

Thus S_5 has the property $\mathbf{P}_8$.

In the case of $\mathrm{SL}(2,5)$ a computer search found the following nonrewritable 8-tuple [13]:

$$\begin{bmatrix}1&0\\1&1\end{bmatrix},\begin{bmatrix}1&1\\0&1\end{bmatrix},\begin{bmatrix}1&0\\2&1\end{bmatrix},\begin{bmatrix}1&2\\0&1\end{bmatrix},$$
$$\begin{bmatrix}0&1\\4&0\end{bmatrix},\begin{bmatrix}1&3\\0&1\end{bmatrix},\begin{bmatrix}1&0\\4&1\end{bmatrix},\begin{bmatrix}1&4\\0&1\end{bmatrix}$$

The nonrewritability of this tuple was checked using CAYLEY.

Lemma 6 (Brandl [5]). *Let H and K be groups which do not have the properties $\mathbf{P}_m$ and $\mathbf{P}_n$ respectively. Then $H \times K$ does not have $\mathbf{P}_{m+n-1}$.*

Proof. Let $h_1, h_2, \ldots, h_m$ and $k_1, k_2, \ldots, k_n$ be nonrewritable tuples in H and K respectively. Then it is clear that the $(m+n-1)$-tuple $(h_1, 1), \ldots, (h_{m-1}, 1)$, $(h_m, k_1), (1, k_2), \ldots, (1, k_n)$ does not rewrite. □

Corollary 7. *If H and K are insoluble groups, then $H \times K$ does not have the property $\mathbf{P}_{13}$.* □

Proof. This follows from Lemma 6 and the fact that no insoluble group has $\mathbf{P}_7$ [4]. □

Lemma 8. *Let G be a group with a nonabelian normal subgroup N. If G has $\mathbf{P}_{m+1}$, then G/N has $\mathbf{P}_m$.* □

This is due to Longobardi and Maj [11]; it is the key to the existence of upper bounds for the derived length of a soluble group with $\mathbf{P}_m$.

Proof of the Theorem. Let G be an insoluble group with $\mathbf{P}_8$. We shall prove a series of assertions about G, culminating in the description contained in the Theorem.

(i) *There is an abelian normal subgroup H such that $\bar{G} = G/H \cong A_5$ or S_5.*

Since soluble subgroups of G have bounded derived length, there is a maximum soluble normal subgroup H of G. Then $\bar{G} = G/H$ is a semisimple group with $\mathbf{P}_8$. By the structure theorem for groups with some $\mathbf{P}_n$ [8], $\bar{G}$ is finite-by-abelian-by-finite. But every finite-by-abelian group is nilpotent-by-finite, so $\bar{G}$ is nilpotent-by-finite. Hence, since $\bar{G}$ is semisimple, it is finite. Let $\bar{R}$ be the completely reducible radical of $\bar{G}$. Since $\bar{R}$ is a direct product of nonabelian simple groups and has the property $\mathbf{P}_8$, it follows on applying Proposition 2 and Corollary 7 that $\bar{R} \cong A_5$. Also $C_{\bar{G}}(\bar{R}) = 1$, so that $\bar{G} \cong A_5$ or S_5. Finally, if H is not abelian, then Lemma 8 shows that $\bar{G}$ has $\mathbf{P}_7$ and hence is soluble. Thus H is abelian.

(ii) *If $\bar{G} \cong A_5$, then $G = H \times K$ where $K \cong A_5$.*

Since A_5 does not have $\mathbf{P}_7$, there are elements $x_1, x_2, \ldots, x_7$ of G such that the 7-tuple $x_1H, x_2H, \ldots, x_7H$ does not rewrite. Let h be an arbitrary element of H. Since G has $\mathbf{P}_8$, the tuple $h, x_1, x_2, \ldots, x_7$ rewrites; therefore

$$hx_1x_2 \cdots x_7 = x_1 \cdots x_{i-1} h x_i \cdots x_7$$

where $1 < i \leq 8$. It follows that h commutes with one of the products $x_1 \cdots x_{i-1}$, $i = 2, 3, \ldots, 8$.

The same argument may be applied to the 8-tuples $x_1, \ldots, x_{r-1}, h, x_r, \ldots, x_7$

for $r = 2, 3, \ldots, 8$. Write $\bar{x}_i = x_i H$ and define subsets of $\bar{G}$

$$S_r = \{\bar{x}_i\bar{x}_{i+1}\cdots\bar{x}_{r-1}, \bar{x}_r\bar{x}_{r+1}\cdots\bar{x}_{k-1} \mid i = 1, 2, \ldots, r-1, \; k = r+1, r+2, \ldots, 8\}$$

for $r = 1, 2, \ldots, 8$. Regarding H as a $\bar{G}$-module via conjugation, we conclude that $G_{\bar{G}}(h) \cap S_r$ is nonempty for $r = 1, 2, \ldots, 8$.

Now comes a crucial computation. We may identify $\bar{x}_1, \ldots, \bar{x}_7$ with the nonrewritable 7-tuple in A_5,

$$(1,2)(3,4), (2,5)(3,4), (1,4)(2,3), (1,2,3,5,4),$$
$$(1,5,4,3,2), (2,4)(3,5), (1,3)(2,4).$$

A simple CAYLEY program constructs the eight subsets S_r and tests each of the subgroups of A_5 for nonempty intersection with every S_r. It emerges that no proper subgroup of A_5 has this property. Therefore $C_{\bar{G}}(h) = \bar{G}$ for each h in H, and thus H is contained in $Z(G)$, the centre of G.

The next step is to consider the possible central extensions of H by $\bar{G}$. Recall that the Schur multiplicator of A_5 has order 2. Thus, if M is a trivial $\bar{G}$-module, the Universal Coefficients Theorem shows that

$$H^2(\bar{G}, M) \cong \mathrm{Hom}(\mathbb{Z}_2, M) \cong M[2],$$

the subgroup of elements of M of order 1 or 2. If H_2 denotes the 2-component of H, then it follows that G/H_2 splits over H/H_2, so $G = HY$ and $H \cap Y = H_2$ for some subgroup Y. Now Y is locally finite and Y/H_2 is finite; hence $Y = H_2 Z$ where Z is a finite subgroup. We claim that Z splits over $B = H_2 \cap Z$. Indeed, if Z/N does not split over B/N where $|B:N| = 2$, then $Z/N \cong \mathrm{SL}(2,5)$ since $Z/B \cong A_5$, which is impossible by Proposition 5. Thus Z/N splits over B/N, and by induction on $|B|$ it follows that Z splits over B, say $Z = B \times K$. Hence $G = HY = HZ = HK$ and $H \cap K = H_2 \cap K = B \cap K = 1$. Therefore $G = H \times K$, H is abelian and $K \cong A_5$.

(iii) Consider now the case where $\bar{G} \cong S_5$.

Let $\bar{N} = N/H \lhd \bar{G}$, with $\bar{N} \cong A_5$ and $|G:N| = 2$. By (ii) $N = H \times K$ where $K \cong A_5$. Notice that $K = G''$, so $K \lhd G$.

The central point to establish is that $H \leq Z(G)$. Since $G/H \cong S_5$, there is a nonrewritable tuple $g_1 H, g_2 H, \ldots, g_7 H$. Now it is possible to choose $g_1, \ldots, g_6$ in N and g_7 not in N; for example, in S_5 the tuple

$$(1,2,5,4,3), (1,2,3), (1,5,4,3,2), (1,2)(4,5),$$
$$(2,3)(4,5), (1,3)(2,4), (1,2)$$

is of this type. Let $h \in H$; then the 8-tuple $g_1, \ldots, g_7, h$ rewrites, from which it follows that h commutes with $g_i g_{i+1} \cdots g_7$ for some $i = 1, 2, \ldots, 7$. Since $g_1, \ldots, g_6 \in N$, we have $[g_j, h] = 1$ for $j = 1, \ldots, 6$, whence $[g_7, h] = 1$. Finally $G = \langle N, g_7 \rangle$, so $h \in Z(G)$.

Let tH be an element of order 2 in $\bar{G}$ which does not belong to $\bar{N}$. Define $H^* = \langle t, H \rangle$, an abelian subgroup. Then $G = H^*K$. Suppose that $t^i h \in K$ for some integer i and $h \in H$; then i must be even, and $t^i \in H$. Thus $t^i h \in H \cap K = 1$, and $H^* \cap K = 1$. Clearly $C_{H^*}(K) = H$ or H^*. Thus G has the desired structure.

Conversely, let $G = H \ltimes K$ with the structure specified in the Theorem. We need to show that G has $\mathbf{P}_8$. Let $x_1, x_2, \ldots, x_8$ be an 8-tuple in G, and write $x_i = h_i k_i$ with $h_i \in H$, $k_i \in K$. Setting $C = C_H(K)$, we have $C \lhd HK = G$, and $G/C \cong A_5$ or S_5. Hence G/C has $\mathbf{P}_8$ by Proposition 5. It follows that there is a nontrivial permutation π such that

$$x_1 x_2 \cdots x_8 = x_{\pi(1)} x_{\pi(2)} \cdots x_{\pi(8)} c$$

for some c in C. Collecting the elements of H to the left in each product, we obtain

$$h_1 h_2 \cdots h_8 u = h_{\pi(1)} h_{\pi(2)} \cdots h_{\pi(8)} v c \,,$$

where $u, v \in K$. Since H is abelian, we deduce that $u = vc$, so $c = v^{-1}u \in H \cap K = 1$. Hence $x_1, x_2, \ldots, x_8$ rewrites and G has $\mathbf{P}_8$. □

4. Constructing insoluble $\mathbf{P}_8$-groups

In conclusion we shall indicate how insoluble groups with $\mathbf{P}_8$ may be constructed. Suppose that $G = HK$ is an insoluble $\mathbf{P}_8$-group, with the notation of the Theorem. There are two possible situations to consider. In the first, every element of G induces an inner automorphism of K by conjugation. In this event $H \leq C_G(K)K$, which leads to $G = C_G(K) \times K = Z(G) \times K$. Thus G is the direct product of an arbitrary abelian group with A_5.

Suppose now that we are in the second situation, i.e. some element of G induces by conjugation an outer automorphism of K. This means that G induces the full group of automorphisms of K, so some g in G induces the automorphism corresponding to conjugation by $(1, 2)$ in A_5. Put $H^* = \langle g, C_G(K) \rangle$, an abelian group since $C_G(K) \leq Z(G)$. Then $G = H^*K$ and $H^* \cap K = 1$; for if $g^i c \in K$ with c in $C_G(K)$, then $g^i \in KC_G(K)$, so i is even, and $g^i \in C_G(K)$; hence $g^i c \in C_G(K) \cap K = 1$. Replacing H by H^* and K by A_5, we may assume that some element h of H induces in K conjugation by $(1, 2)$. Notice that $|H : C_H(K)| = 2$.

Conversely, suppose that we are given an abelian group H and a subgroup H_0 with index 2 in H. There is a unique homomorphism $\xi : H \to S_5$ with kernel H_0

and image $\langle (1,2) \rangle$. Identifying $\mathrm{Aut}(A_5)$ with S_5, we may form the semidirect product determined by ξ,

$$G(H, H_0) = H \ltimes_{\xi} K,$$

where $K = A_5$. If $h \in H \backslash H_0$, then h induces by conjugation in K the automorphism arising from conjugation by $(1,2)$, an outer automorphism. Clearly $G(H, H_0)$ is an insoluble group with $\mathbf{P}_8$ of the second type, and every such group is isomorphic with some $G(H, H_0)$. Notice that $Z(G(H, H_0)) = H_0$.

Finally, it is routine to prove that $G(H, H_0) \cong G(\bar{H}, \bar{H}_0)$ if and only if there is an isomorphism $\alpha : H \to \bar{H}$ such that $H_0^{\alpha} = \bar{H}_0$. Thus $G(H, H_0)$ is determined to within isomorphism by the isomorphism type of H and the $\mathrm{Aut}(H)$-orbit of H_0 in H.

Acknowledgment

We wish to thank Professor Roy Campbell of the Department of Computer Science at the University of Illinois in Urbana-Champaign for facilitating access to advanced computing equipment, and for his interest in our project. We owe a special debt to Arch Robison of the same department for upgrading our original PASCAL program and translating into C++. Finally, we acknowledge use of computing facilities at St. Louis University and at the Symbolic Computation Laboratory at the University of Illinois in Urbana-Champaign.

References

[1] M. Aschbacher, Finite Group Theory (Cambridge University Press, Cambridge, 1986).
[2] R.D. Blyth, Rewriting products of group elements—II, J. Algebra 119 (1988) 246–259.
[3] R.D. Blyth and D.J.S. Robinson, Recent progress on rewritability in groups, in: Group Theory, Proceedings of the 1987 Singapore Conference (de Gruyter, Berlin, 1989).
[4] R.D. Blyth and D.J.S. Robinson, Solution of the solubility problem for rewritable groups, J. London Math. Soc. (2) 41 (1991) 438–444.
[5] R. Brandl, General bounds for permutability in finite groups, Arch. Math. 53 (1989) 245–249.
[6] R.W. Carter, Simple Groups of Lie Type (Wiley, London, 1972).
[7] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, ATLAS of Finite Groups (Clarendon Press, Oxford, 1985).
[8] M. Curzio, P. Longobardi, M. Maj and D.J.S. Robinson, A permutational property of groups, Arch. Math. (Basel) 44 (1985) 385–389.
[9] B. Huppert, Endliche Gruppen, Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen 134 (Springer, Berlin, 1967).
[10] B. Huppert and N. Blackburn, Finite Groups III, Grundlehren der Mathematischen Wissenschaften 243 (Springer, Berlin, 1982).
[11] P. Longobardi and M. Maj, On the derived length of groups with some permutational property, Preprint.
[12] P. Longobardi, M. Maj and S.E. Stonehewer, Classification of groups in which every product of four elements can be reordered, Preprint.

[13] A.D. Robison, An improved rewriting-number algorithm, BIT 30 (1990) 51–61.
[14] G.M. Seitz, Generation of finite groups of Lie type, Trans. Amer. Math. Soc. 271 (1982) 351–407.
[15] M. Suzuki, On a class of doubly transitive groups, Ann. of Math. 75 (1962) 105–145.
[16] J. Tits, Les groupes simples de Suzuki et de Ree, Sém. Bourbaki 13 (1960/61) exposé 210.